

日本国特許庁

19.05.03

JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日

Date of Application:

2002年 4月11日

出願番号

Application Number:

特願2002-109714

[ST.10/C]:

[JP2002-109714]

出願人

Applicant(s):

インターナショナル・ビジネス・マシーンズ・コーポレーション

REC'D 06 JUN 2003

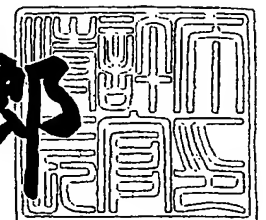
WIPO PCT

PRIORITY  
DOCUMENTSUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2003年 4月11日

特許庁長官  
Commissioner,  
Japan Patent Office

太田信一郎



出証番号 出証特2003-3025464

【書類名】 特許願

【整理番号】 JP9020047

【提出日】 平成14年 4月11日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/00

【発明者】

    【住所又は居所】 神奈川県大和市下鶴間 1 6 2 3 番地 1 4 日本アイ・ピー・エム株式会社 大和事業所内

    【氏名】 尾家 正樹

【特許出願人】

    【識別番号】 390009531

    【氏名又は名称】 インターナショナル・ビジネス・マシーンズ・コーポレーション

【代理人】

    【識別番号】 100086243

    【弁理士】

    【氏名又は名称】 坂口 博

【代理人】

    【識別番号】 100091568

    【弁理士】

    【氏名又は名称】 市位 嘉宏

【代理人】

    【識別番号】 100106699

    【弁理士】

    【氏名又は名称】 渡部 弘道

【復代理人】

    【識別番号】 100104880

    【弁理士】

    【氏名又は名称】 古部 次郎

【選任した復代理人】

【識別番号】 100100077

【弁理士】

【氏名又は名称】 大場 充

【手数料の表示】

【予納台帳番号】 081504

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9706050

【包括委任状番号】 9704733

【包括委任状番号】 0004480

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンピュータ装置、コンピュータ装置のセキュリティ設定  
方法、プログラム

【特許請求の範囲】

【請求項 1】 他のデバイスとの間で通信可能なコンピュータ装置であって

前記他のデバイスとの通信を介し当該他のデバイスの識別情報を取得する識別  
情報取得手段と、

取得した前記識別情報に基づいて、前記コンピュータ装置の使用環境を判定す  
る使用環境判定手段と、

判定された前記コンピュータ装置の使用環境に基づき、当該コンピュータ装置  
の設定を変更する設定変更手段と、  
を備えることを特徴とするコンピュータ装置。

【請求項 2】 前記使用環境判定手段は、前記識別情報に基づき、前記コン  
ピュータ装置の周囲に存在する前記他のデバイスを特定することによって当該コ  
ンピュータ装置の使用環境を判定することを特徴とする請求項 1 記載のコンピ  
ュータ装置。

【請求項 3】 前記コンピュータ装置は、ブルートゥースによる通信を行う  
通信手段をさらに備え、

前記識別情報取得手段は、ブルートゥースによる通信が可能な前記他のデバイ  
スからブルートゥース・デバイス・アドレスを前記識別情報として取得すること  
を特徴とする請求項 2 記載のコンピュータ装置。

【請求項 4】 前記設定変更手段は、前記コンピュータ装置の使用環境に基  
づき、当該コンピュータ装置のセキュリティ設定を変更することを特徴とする請  
求項 1 記載のコンピュータ装置。

【請求項 5】 前記設定変更手段は、前記使用環境判定手段にて特定の使用  
環境にあると判定されたときには当該特定の使用環境に応じたセキュリティ設定  
とし、

前記特定の使用環境以外であると判定されたときには、前記特定の使用環境の

ときよりも高いセキュリティ性を有したセキュリティ設定とすることを特徴とする請求項 4 記載のコンピュータ装置。

【請求項 6】 前記設定変更手段は、前記コンピュータ装置の使用環境に基づき、当該コンピュータ装置における消費電力を制御するための設定を変更することを特徴とする請求項 1 記載のコンピュータ装置。

【請求項 7】 可搬性を有するコンピュータ装置が当該コンピュータ装置の使用環境に関する情報を取得するステップと、

取得した前記情報に基づいて前記コンピュータ装置が当該コンピュータ装置のセキュリティ設定を変更するステップと、  
を有することを特徴とするコンピュータ装置のセキュリティ設定方法。

【請求項 8】 前記使用環境に関する情報を取得するステップでは、前記コンピュータ装置の周囲のデバイスから発せられる当該デバイスの識別情報を取得することを特徴とする請求項 7 記載のコンピュータ装置のセキュリティ設定方法。

【請求項 9】 前記セキュリティ設定を変更するステップでは、前記デバイスの識別情報が予め登録されたものであるか否かに応じ、セキュリティ設定のレベルを変更することを特徴とする請求項 8 記載のコンピュータ装置のセキュリティ設定方法。

【請求項 10】 前記デバイスの識別情報が予め登録されたものではないとき、セキュリティ設定を高いレベルに変更することを特徴とする請求項 9 記載のコンピュータ装置のセキュリティ設定方法。

【請求項 11】 可搬性を有するコンピュータ装置が当該コンピュータ装置のセキュリティ設定を行う方法であって、

前記コンピュータ装置と通信可能な状態にあるデバイスに関するデバイス情報を取得するステップと、

前記デバイス情報が取得できる環境におけるセキュリティ設定の指定を受け付けるステップと、

指定された前記セキュリティ設定を前記デバイス情報に関連付けて格納するステップと、

を有することを特徴とするコンピュータ装置のセキュリティ設定方法。

【請求項 1 2】 前記セキュリティ設定および前記デバイス情報の格納後、前記コンピュータ装置と通信可能な状態にあるデバイスに関するデバイス情報を取得するステップと、

取得した前記デバイス情報に関連付けられた前記セキュリティ設定を呼び出すステップと、

前記コンピュータ装置を、呼び出した前記セキュリティ設定に変更するステップと、

をさらに前記コンピュータ装置が実行することを特徴とするコンピュータ装置のセキュリティ設定方法。

【請求項 1 3】 コンピュータ装置に所定の処理を実行させるプログラムであって、

前記コンピュータ装置の周囲に存在する他のデバイスとのブルートゥースによる通信を介し、当該デバイスのアドレス情報を取得する処理と、

取得した前記アドレス情報に基づいて、前記コンピュータ装置の設定を変更する処理と、

を有することを特徴とするプログラム。

【請求項 1 4】 前記コンピュータ装置の設定を変更する処理では、当該コンピュータ装置のセキュリティ設定を変更することを特徴とする請求項 1 3 記載のプログラム。

【請求項 1 5】 前記コンピュータ装置の設定を変更する処理では、前記アドレス情報が予め登録されたものであるか否かに応じ、前記セキュリティ設定のレベルを変更することを特徴とする請求項 1 4 記載のプログラム。

【請求項 1 6】 前記コンピュータ装置の設定を変更する処理では、前記デバイスのアドレス情報が予め登録されたものではないとき、前記セキュリティ設定を高いレベルに変更することを特徴とする請求項 1 5 記載のプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、可搬性のあるコンピュータ装置に関し、例えばセキュリティ設定等を行うに際して用いて好適な技術に関する。

#### 【0002】

##### 【従来の技術】

近年、ノートブック型のPC、PDA(Personal Digital Assistants)等、可搬性のあるいわゆるモバイル機器が広く用いられている。

ノートブック型のPC(以下、単にPCと称する)を例に挙げると、ユーザは、例えばオフィスで無線LANを用いてネットワークに接続していたPCを、自宅に持ち帰ってモデムを用いてアナログ電話回線を介してネットワークに接続し、さらに出先では携帯電話を介してネットワークに接続したりしている。

また、最近では、駅や繁華街等の特定のエリアに無線LAN環境が提供され、このようなエリア内では、提供された無線LANを用いてネットワークに接続することもできるようになっている。

さらに、ブルートゥースといった短距離無線通信技術も広まりつつあり、オフィス、自宅、出先等において、モデムやLANアクセスポイント、あるいは他のデバイスとの間でブルートゥースによってデータ通信を行うこともできるようになっている。

#### 【0003】

##### 【発明が解決しようとする課題】

しかしながら、上記のように、1台のPCにおいて、オフィス、自宅(以下、これをホームと適宜称する)、出先(以下、これをモバイルと適宜称する)と使用環境が複数種にわたる場合、それぞれの場所に移動するたびに、少なくともネットワークに接続するための各種設定を行わなければならない。

この設定には、数項目から数十項目の設定を変更しなければならないため、言うまでもなく非常に面倒であり、設定の変更内容を誤った場合には、ネットワーク接続自体ができなくなってしまうという問題がある。

#### 【0004】

このような問題を解決するため、タスクバー等に表示されるユーティリティ上において使用環境を選択するだけで、設定がワンタッチで切り替えられるような

ものも一部で提供されている。これにより、予めそれぞれの使用環境に応じた設定をしておけば良いので、毎回面倒な設定を行う必要がなくなる。

しかし、例えば、実際にはオフィスなのにホームの設定を選択する等、ユーザが設定の変更先を誤った場合には、ネットワーク接続ができないという問題が生じる。さらに、ネットワーク接続ができたとしても、実際には出先で、セキュリティ性の高いモバイルの設定とすべき使用環境にあるのに、セキュリティ性の低いホームの設定となっている場合等、誤った設定でPCを使用し続けると、潜在的なセキュリティホールとなる可能性もあり、これは重要な問題である。

このようなセキュリティホールがあると、特に、無線LANやブルートゥースを用いてネットワーク接続するような環境では、他人のデバイスからの不正アクセスを有効に防ぐことができなくなってしまうこともあるからである。

#### 【0005】

本発明は、このような技術的課題に基づいてなされたもので、使用環境に応じて確実に設定変更を行うことのできる技術を提供することを主たる目的とする。

また、他の目的は、よりセキュリティ性の高いネットワーク接続環境を常に確保することにある。

#### 【0006】

##### 【課題を解決するための手段】

かかる目的のもと、本発明のコンピュータ装置は、他のデバイスとの通信を介して識別情報取得手段にて取得した他のデバイスの識別情報に基づき、使用環境判定手段にてコンピュータ装置の使用環境を判定する。そして、判定された使用環境に基づき、設定変更手段にて、例えばセキュリティ設定等、コンピュータ装置の設定を変更する。

このとき、使用環境判定手段では、識別情報に基づき、コンピュータ装置の周囲に存在する他のデバイスを特定することによってコンピュータ装置の使用環境を判定することができる。

また、コンピュータ装置がブルートゥースによる通信を行う通信手段を備える場合、識別情報取得手段では、ブルートゥースによる通信が可能なデバイスに対して個別に割り当てられるブルートゥース・デバイス・アドレスを、他のデバイ



スから識別情報として取得することができる。

ここで、設定変更手段では、コンピュータ装置が、例えばホームやオフィス等、特定の使用環境にあると判定されたときには、その特定の使用環境に応じたセキュリティ設定とし、出先等、特定の使用環境以外であると判定されたときには、特定の使用環境のときよりも高いセキュリティ性を有したセキュリティ設定とするのが好ましい。

また、設定変更手段では、コンピュータ装置の使用環境に基づき、コンピュータ装置における消費電力を制御するための設定を変更することもできる。

#### 【0007】

本発明のコンピュータ装置のセキュリティ設定方法は、コンピュータ装置の使用環境に関する情報を取得し、これに基づいてコンピュータ装置のセキュリティ設定を変更することを特徴とする。

使用環境に関する情報を取得するに際しては、コンピュータ装置の周囲のデバイスから発せられるデバイスの識別情報を取得することができる。また、これ以外に、コンピュータ装置がGPS (Global Positioning System: 全地球測位システム) 等を利用可能であれば、GPSによって測位される位置情報を、コンピュータ装置の使用環境に関する情報として取得することもできる。

また、セキュリティ設定を変更するに際しては、デバイスの識別情報が予め登録されたものであるか否かに応じ、セキュリティ設定のレベルを変更することができる。デバイスの識別情報が予め登録されたものではないとき、セキュリティ設定を高いレベルに変更するのである。

#### 【0008】

また、本発明は、コンピュータ装置と通信可能な状態にあるデバイスに関するデバイス情報を取得し、そのデバイス情報が取得できる環境におけるセキュリティ設定を指定するための外部からの入力を受け付けると、指定されたセキュリティ設定をデバイス情報に関連付けて格納することを特徴とするコンピュータ装置のセキュリティ設定方法として捉えることができる。

このような方法では、セキュリティ設定およびデバイス情報の格納後に、コンピュータ装置と通信可能な状態にあるデバイスに関するデバイス情報を取得し、

取得したデバイス情報に関連付けられたセキュリティ設定を呼び出し、呼び出したセキュリティ設定に変更することができる。

【 0 0 0 9 】

本発明は、コンピュータ装置に所定の処理を実行させるプログラムとして捉えることもできる。この場合、このプログラムは、コンピュータ装置の周囲に存在する他のデバイスとのブルートゥースによる通信を介し、他のデバイスのアドレス情報を取得する処理と、取得したアドレス情報に基づいてコンピュータ装置のセキュリティ設定等を変更する処理と、を有する。

【 0 0 1 0 】

ここで、本発明におけるコンピュータ装置は、P Cに限らず、P D Aや、携帯電話端末、他の各種デバイスであっても良いことは言うまでも無い。

【 0 0 1 1 】

【発明の実施の形態】

以下、添付図面に示す実施の形態に基づいてこの発明を詳細に説明する。

図 1 は、本実施の形態におけるノートブック型の P C (コンピュータ装置) 1 0 のデバイス構成を説明するための図である。

この図 1 に示すように、P C 1 0 は、所定の制御プログラムに基づいた処理を実行する C P U 1 1、処理用データを格納する R A M (Random Access Memory) 等のメモリ 1 2、ディスプレイ部 (L C D) 1 3 に表示する画像を制御するグラフィックチップ 1 4 が、チップセット 1 5 に接続されている。

【 0 0 1 2 】

このチップセット 1 5 は、ブリッジ回路 1 6 に接続されている。

このブリッジ回路 1 6 には、I D E チャンネル 1 7 を介して H D D 1 8 が接続される。

また、ブリッジ回路 1 6 には、キーボード 1 9 や図示しないマウス等のポインティングデバイスからの信号の入力に基づいたイベントを出力するコントローラ 2 0、B I O S (Basic Input/Output System) を格納した E E P R O M (Electrically Erasable and Programmable ROM) 2 1 が接続されており、キーボード 1 9 やポインティングデバイスからの入力に応じ、B I O S が、P C 1 0 の各部を制

御する構成となっている。

加えて、このブリッジ回路16は、各種の設定情報を記憶するCMOS (Complementary Metal Oxide Semiconductor) 22を内蔵し、CMOS 22はバッテリー23によって、常時電源が供給されるようになっている。

#### 【0013】

また、ブリッジ回路16には、USB (Universal Serial Bus) 24を介し、ブルートゥース通信コントローラ(識別情報取得手段、通信手段)30が接続され、PCI (Peripheral Component Interconnect)バス25を介し、有線LAN通信コントローラ31、無線LAN通信コントローラ32、モデム33が接続されている。

ブルートゥース通信コントローラ30は、アンテナ34を介し、他のブルートゥース対応のデバイスとの間で短距離無線通信によるデータ通信を制御する。このブルートゥース通信コントローラ30では、アンテナ34で送受信する電波が届く範囲内(一般に10～100m以内)に存在する他のブルートゥース対応のデバイスとの通信を制御する。また、ブルートゥース対応のデバイスは、電源が入っている限り、ブルートゥース・デバイス・アドレス(以下、BDアドレス)を含む電波を発している。ブルートゥース通信コントローラ30は、アンテナ34で受信した電波にBDアドレスが含まれる場合、これを検出する機能を備えている。

#### 【0014】

また、有線LAN通信コントローラ31は、ジャック35に接続したLANケーブル(図示無し)を介して有線で外部のネットワーク50にアクセスし、ネットワーク50を介した他のコンピュータ装置とのデータ通信を制御する。

無線LAN通信コントローラ32は、アンテナ36を介して無線で外部のネットワーク50にアクセスし、ネットワーク50を介した他のコンピュータ装置とのデータ通信を制御する。

また、モデム33は、ジャック37に接続したケーブル(図示無し)からアナログ回線網を介してネットワーク50にアクセスし、ネットワーク50を介した他のコンピュータ装置とのデータ通信を制御する。

これにより、PC10は、例えば、ブルートゥース、無線LAN、有線LAN、アナログ電話回線を介したネットワーク接続が可能な構成となっている。

#### 【0015】

ここで、有線LAN通信コントローラ31と無線LAN通信コントローラ32は、実際には一つのイーサネットチップによって実現されるものであっても良い。また、ブルートゥース通信コントローラ30、有線LAN通信コントローラ31、無線LAN通信コントローラ32、モデム33の全てが必須ではなく、少なくともブルートゥース通信コントローラ30を備えていればネットワーク通信機能を備えることができる。さらに、有線LAN通信コントローラ31、無線LAN通信コントローラ32、モデム33のいずれも装備しない場合は、ブルートゥース通信コントローラ30において短距離無線通信によってLANアクセスポイントにアクセスし、このLANアクセスポイントからネットワーク50にアクセスさせる構成とすることが可能である。

#### 【0016】

このような構成を有するPC10は、ブルートゥース通信コントローラ30の有する、電波の届く範囲内に存在する他のデバイスを認識する機能を用い、周辺に位置するデバイスの種類等からPC10の使用環境を判定し、使用環境に応じたセキュリティ設定等を自動的に行う。

図2は、上記のようなデバイス構成を有するPC10を、機能的な構成で捉えた図である。この図2に示すように、PC10は、予めインストールされたプログラムに基づいた処理をCPU(図示無し)が実行することによって実現される機能として、環境判定部(使用環境判定手段)40、通信設定制御部41、セキュリティ設定制御部(設定変更手段)42、省電力設定制御部(設定変更手段)43を備える。

環境判定部40は、ブルートゥース通信コントローラ30においてブルートゥースによる通信が可能なデバイスに関する情報を収集することによって、PC10の使用環境を判定する。

通信設定制御部41は、環境判定部40で判定した使用環境に合わせたネットワーク通信設定を行う。

セキュリティ設定制御部 4 2 は、環境判定部 4 0 で判定した使用環境に合わせたセキュリティ設定を行う。このときには、予め複数段階のセキュリティ設定に関する情報が、HDD 1 8 に格納されたデータによって実現されるセキュリティ設定情報格納部 4 4 に格納されており、セキュリティ設定制御部 4 2 では、この情報を参照することによって、使用環境に応じたセキュリティ設定を行う。

省電力設定制御部 4 3 では、PC 1 0 の使用環境に応じ、CPU 1 1 の動作速度やモニタ 1 3 の表示を制御したり、サスペンドモードやハイバネーションモードへの移行等を制御する。

#### 【 0 0 1 7 】

ここで、PC 1 0 の使用環境の例を挙げる。

図 3 は、ユーザが自宅等で PC 1 0 を使用する場合は、後に本実施の形態で「ホーム」と称するセキュリティレベルを設定する使用環境である。

ユーザが自宅で PC 1 0 を使用する場合には、ブルートゥース用の電波が届く範囲内に、他のデバイスとして、ブルートゥース対応のプリンタ 1 0 0、モデム 1 0 1 が存在するものとする。

また、図 4 は、ユーザが勤務先のオフィス等で PC 1 0 を使用する場合は、後に本実施の形態で「オフィス」と称するセキュリティレベルを設定する使用環境である。

ユーザがオフィスで PC 1 0 を使用する場合には、ブルートゥース用の電波が届く範囲内に、他のデバイスとして、ブルートゥース対応のプリンタ 2 0 0、プロジェクタ 2 0 1、ネットワーク 5 0 にアクセスするための LAN アクセスポイント 2 0 2 が存在するものとする。

図 5 は、ユーザが出先に PC 1 0 を持ち出して使用する場合は、本実施の形態で後に「モバイル」と称するセキュリティレベルを設定する使用環境である。

ここで、ユーザが出先で PC 1 0 を使用する場合は、ブルートゥース用の電波が届く範囲内に、他のデバイスとして、自らが使用する他のブルートゥース対応のデバイスは所持していないものとする。すると、特に電車内や繁華街、コーヒESHOP等で、PC 1 0 のブルートゥース用の電波が届く範囲内に、他人が所持するブルートゥース対応の、携帯電話端末 3 0 0、PC 3 0 1 (この PC 3 0 1

は上記PC10と同じ構成である必要はない)、PDA302等が存在することがある。

#### 【0018】

次に、上記のような、「ホーム」、「オフィス」、「モバイル」といった複数のセキュリティレベルの例を挙げる。

ここで、ブルートゥースによる通信を行う際には、セキュリティ設定として、「認証(Authentication)」、「許可(Authorization)」、「暗号化(Encryption)」の3項目がある。

「認証」とは、パス・キーと称される手入力によるキーワードの入力、あるいはリンク・キーと称される、パス・キーに基づいて自動的に生成されるキーワードにより、ブルートゥースによる通信を行うデバイス間で、相互認証を行うものである。

「許可」とは、ファイル転送や名刺交換といったサービスを行う毎にアクセスの可否をコントロールするものである。

「暗号化」とは、デバイス間でデータを転送する際に、リンク・キーから生成される暗号鍵を用い、データを暗号化するものである。

#### 【0019】

図6は、セキュリティレベルの設定の例を示すもので、「ホーム」<「オフィス」<「モバイル」の順でセキュリティ性が高くなり、PC10から外部資源へのアクセス・外部資源からPC10へのアクセスの困難性が高くなる、つまりPC10におけるアクセス制限が厳しくなる設定となっている。

セキュリティレベルが「ホーム」の場合、他のデバイスからPC10に対する接続を行うときには、デバイスの「認証」を必須とし、「許可」については必要に応じて行い、データの「暗号化」は必須とする。また、PC10から他のデバイスに対して接続するときには、デバイスの「認証」、「許可」、「暗号化」は、他のデバイス側から要求があったときに行うものとする。

セキュリティレベルが「オフィス」の場合、他のデバイスからPC10に対する接続を行うときには、業務上等で機密度の高いデータをやり取りすることが想定できるため、ここでは、デバイスの「認証」および「許可」、データの「暗号

化」を必須とする。また、PC10から他のデバイスに対して接続するときには、デバイスの「認証」、「許可」、「暗号化」は、他のデバイス側から要求があったときに行うものとする。

セキュリティレベルが「モバイル」の場合、出先等では、最も高いセキュリティを確保する必要があるため、他人のデバイスからのアクセスについては、全て「拒否」する。また、PC10から他のデバイスに対して接続するときには、デバイスの「認証」、「許可」、「暗号化」を必須とする。

図6に示したようなセキュリティレベルの設定は、ユーザが予め各項目の設定内容を選択することによって設定しても良いし、また予め上記のような複数段階のセキュリティレベルをデフォルトで用意しておいてもよい。

#### 【0020】

さて、ユーザは、自らがPC10を使用する使用環境に応じ、上記のようなセキュリティレベルの中から任意の段階を選択し、設定しておく必要がある。

これには、使用環境に応じたセキュリティ設定を行うためのアプリケーションを起動させる。

すると、図7に示すように、このアプリケーションでは、PC10のブルートゥース通信コントローラ30において、ブルートゥース用の電波が届く範囲内に存在するデバイスを検索する(ステップS101)。このとき、ブルートゥース用の電波が届く範囲内にブルートゥース対応のデバイスが存在していれば、そのデバイス自身の識別情報、デバイス情報、アドレス情報となるBDアドレスを検出(捕捉)することができる。

#### 【0021】

PC10では、他のデバイスから発せられるBDアドレスを捕捉することによって、周囲に存在するデバイスを確定する(ステップS102)。

続いて、必要に応じ、PC10では、モニタ13上に、BDアドレスを捕捉したデバイスに関する情報を表示し、ユーザに確認を促すこともできる。このようにすれば、その時点で捕捉されたデバイスのうち、常時電源が入っているような特定のデバイスのみをユーザが選択することもできる。

PC10は、さらに、ユーザに対し、その場所におけるPC10のセキュリテ

イレベルの設定を促す表示をモニタ13上に行う(ステップS103)。

#### 【0022】

ユーザは、その場所(使用環境)におけるPC10のセキュリティレベルを、図6に示したような複数段階の設定の中から選択し、これを入力する。

PC10では、入力されたセキュリティレベルの選択を受け付け、これを、検出されたデバイスのBDアドレスと関連付けてHDD18等に格納することにより、セキュリティレベルの設定を登録する(ステップS104)。

例えば、図3に示したように、プリンタ100、モデム101のBDアドレスが検出された使用環境に対し、ユーザが選択した「ホーム」というセキュリティレベルの設定を登録するのである。また、図4に示したように、プリンタ200、プロジェクタ201、LANアクセスポイント202が検出される使用環境では、ユーザが選択した「オフィス」というセキュリティレベルの設定を関連付けて登録する。

ところで、図7の一連の処理によって実行されるセキュリティ設定処理は、「ホーム」や「オフィス」等、ユーザがたびたび訪れる特定の場所においてのみ行えばよい。

そして、それ以外の使用環境では、「モバイル」のセキュリティレベルとするよう、ユーザが設定を行っても良いし、デフォルトでそのような設定としておいてもよい。

#### 【0023】

また、上記の処理において、それぞれの使用環境に応じ、ネットワーク50を介した通信を行うための設定や、プリンタ100や200に応じた設定を記憶しておくこともできる。例えば、図3の例ではモデム101を用いるための各種設定情報、図4の例では、LANアクセスポイント202を用いるための各種設定情報等である。

さらに、上記の処理において、それぞれの使用環境に応じた、省電力機能の設定を行うこともできる。例えば、セキュリティレベルとして「モバイル」が設定されるような使用環境では、消費電力をセーブするため、CPU11の処理速度やHDD18の回転速度を落としたり、PC10を持ち歩く際には使用しないA



Cアダプタの制御にのみ必要な部品への電源供給を遮断したりする等、省電力効果が最も高い設定とすることができる。

#### 【0024】

上記のように、使用環境に応じたセキュリティ設定を行った後は、PC10が、以下のような処理を自動的に実行することにより、使用環境に応じたセキュリティ設定の切り替えを行う。

図8に示すように、PC10では、システムの起動時、あるいはユーザの所定の操作によって要求がなされた時、あるいは予め設定されたタイマーによる割込み要求があった時に、PC10のブルートゥース通信コントローラ30において、ブルートゥース用の電波が届く範囲内に存在するデバイスを検索する(ステップS201)。すると、ブルートゥース用の電波が届く範囲内に存在するデバイスのBDアドレスを捕捉することができる。

#### 【0025】

続いて、PC10の環境判定部40にて、捕捉されたBDアドレスに基づき、その時点でのPC10の使用環境を判定する。

これにはまず、「ホーム」のセキュリティレベルに関連付けられているBDアドレスが、検出されたBDアドレスに含まれているか否かを判断する。つまり、セキュリティレベルを「ホーム」と設定すべき使用環境にあるデバイスが存在するか否かを判断するのである(ステップS202)。

その結果、「ホーム」のセキュリティレベルに関連付けられているBDアドレスが、検出されたBDアドレスに含まれていれば、環境判定部40では、PC10がセキュリティレベルを「ホーム」とすべき使用環境にあると判断する。すると、セキュリティ設定制御部42では、PC10のブルートゥース通信コントローラ30において実行するブルートゥース通信に際するセキュリティレベルの設定を、「ホーム」に変更する(ステップS203)。また、通信設定制御部41では、ネットワーク50を介した通信を行うためのPC10側の通信設定等を、BDアドレスを検出したデバイス(図3の例ではモデム101)に応じたものに変更することもできる。さらに、PC10側のプリンタ設定を、BDアドレスを検出したデバイス(図3の例ではプリンタ100)に応じたものに自動的に変更するこ

ともできる。

#### 【0026】

検出されたBDアドレスに、「ホーム」のセキュリティレベルの設定に関連付けられているBDアドレスが含まれていない場合、続いて、「オフィス」のセキュリティレベルに関連付けられているBDアドレスが、検出されたBDアドレスに含まれているか否かを判断する。つまり、セキュリティレベルを「オフィス」と設定すべき使用環境にあるデバイスが存在するか否かを判断するのである(ステップS204)。

その結果、「オフィス」のセキュリティレベルに関連付けられているBDアドレスが、検出されたBDアドレスに含まれていれば、環境判定部40では、PC10がセキュリティレベルを「オフィス」とすべき使用環境にあると判断する。すると、セキュリティ設定制御部42では、PC10のブルートゥース通信コントローラ30において実行するブルートゥース通信に際するセキュリティレベルの設定を、「オフィス」に変更する(ステップS205)。また、通信設定制御部41では、ネットワーク50を介した通信を行うためのPC10側の通信設定等を、BDアドレスを検出したデバイス(図4の例ではLANアクセスポイント202)に応じたものに変更することもできる。さらに、PC10側のプリンタ設定やプロジェクタ設定を、BDアドレスを検出したデバイス(図4の例ではプリンタ200やプロジェクタ201)に応じたものに自動的に変更することもできる。

#### 【0027】

さらに、検出されたBDアドレスに、「オフィス」のセキュリティレベルの設定に関連付けられているBDアドレスが含まれていない場合は、環境判定部40では、PC10が、セキュリティレベルを「モバイル」とすべき使用環境にあると判断する。すると、セキュリティ設定制御部42では、PC10のブルートゥース通信コントローラ30において実行するブルートゥース通信に際するセキュリティレベルの設定を、「モバイル」に変更する(ステップS206)。また、省電力設定制御部43では、省電力効果の最も高い設定への変更を行うこともできる。

## 【 0 0 2 8 】

上述したような構成によれば、P C 1 0 では、ブルートゥースを用い、周辺に存在するデバイスを検索することによって、P C 1 0 の使用環境を判定し、その使用環境に応じてセキュリティレベルの設定を自動的に変更することができる。これにより、使用環境に応じたセキュリティレベルの変更を確実に行うことが可能となるので、常に最適なセキュリティ環境を確保することが可能となる。しかも、ユーザは、P C 1 0 の使用環境が変わる毎にセキュリティ設定を変更する必要がなくなるので、P C 1 0 の使い勝手が向上する。

さらに、使用環境を判定する処理においては、使用環境を判定する処理において、セキュリティレベルを「ホーム」や「オフィス」とすべき使用環境に P C があるときであっても、無線の状態等によってその使用環境に存在すべきデバイスが検出されないときには、セキュリティ性の高い「モバイル」のセキュリティレベルに設定するようにした。これにより、フェイルセーフ機能を有していると言える。

この他、判定された使用環境に応じ、ネットワーク通信を行うための設定や、省電力設定、プリンタ設定やプロジェクタ設定等についても、同様に自動的に変更することが可能であるので、この点においても、P C 1 0 の使い勝手を大幅に向上させることができる。

さらに、上記のような設定を行うに際し、ブルートゥースを用いるようにした。ブルートゥースの場合、周囲のデバイスの電源が入っていさえいれば、実際に P C 1 0 と周囲との間でデータ通信を行わなくてもよいので、特にセキュリティ設定を「モバイル」とするような使用環境においても、他のデバイスに P C 1 0 自身の情報を通知する必要も無く、高いセキュリティ性を保ったまま、上記効果を奏することができる。

## 【 0 0 2 9 】

なお、上記実施の形態では、図 6 にセキュリティレベルの例を挙げたが、あくまでもこれは一例に過ぎず、より少ない 2 段階、あるいは、より多い 4 段階以上のセキュリティレベルの設定とすることも可能であるし、「ホーム」、「オフィス」、「モバイル」といった各セキュリティレベルの内容も適宜変更することが

可能である。

また、例えば、勤務先におけるユーザの自席と、ユーザが使用する会議室等、複数の使用環境において、同じ「オフィス」のセキュリティ設定とすることも可能である。このような場合、通信設定や省電力設定については、個々の使用環境に応じた設定内容を記憶しさえすれば、使用環境に応じて設定を自動的に変更することは可能である。

#### 【0030】

ところで、上記実施の形態においては、使用環境を特定するために、ブルートゥースを用い、各デバイスに固有に割り当てられるBDアドレスを用いる構成としたが、これに限るものではない。

他に、PC10がデータ通信を行う際に他のデバイス等とやり取りする、IPアドレスや、無線や携帯電話通信網を用いる際の基地局アドレス、MACアドレス等を用いることも可能である。IPアドレスやMACアドレスの場合には、上記と同様に周辺のデバイスを特定することによって使用環境を判定することになる。また、無線や携帯電話通信網を用いる際の基地局アドレスを捕捉する場合には、実質的には基地局を特定することによってPC10が使用されている場所を特定し、これによって使用環境に応じたセキュリティ設定等を行うことになる。

ところで、IPアドレスを用いる場合、IPアドレスを動的に割り振る場合であっても、オフィスのフロア等、特定のエリアまでは絞り込むことができるので、これによってPC10の使用環境を判定すればよい。また、IPアドレスの場合、使用環境を特定するという主旨からしても、汎用的に用いられるアドレス以外の、固有のIPアドレスを設定しておくのが好ましい。

また、基地局アドレスの場合のように、PC10の使用場所を特定するという観点からすれば、PC10にGPS(Global Positioning System)を用い、PC10の位置を測位することによってPC10の使用環境を判定することも考えられる。

#### 【0031】

また、上記実施の形態で示したような、使用環境に応じたセキュリティ設定等を自動的に変更するためのプログラムは、以下のような記憶媒体の形態とするこ

ともできる。

すなわち、記憶媒体としては、コンピュータ装置に実行させる上記したようなプログラムを、CD-ROM、DVD、メモリ、ハードディスク等の記憶媒体に、コンピュータ装置が読み取り可能に記憶させれば良い。

これ以外にも、本発明の主旨を逸脱しない限り、上記実施の形態で挙げた構成を取捨選択したり、他の構成に適宜変更することが可能である。

#### 【0032】

##### 【発明の効果】

以上説明したように、本発明によれば、使用環境に応じて確実に設定変更を行うことができ、セキュリティ性の高いネットワーク接続環境を常に確保することが可能となる。

##### 【図面の簡単な説明】

【図1】 本実施の形態におけるコンピュータ装置の構成を示す図である。

【図2】 コンピュータ装置の、ブルートゥースを用いた設定制御に関わる構成を抽出した図である。

【図3】 セキュリティ設定を「ホーム」とするときのコンピュータ装置の使用環境の一例を示す図である。

【図4】 セキュリティ設定を「オフィス」とするときのコンピュータ装置の使用環境の一例を示す図である。

【図5】 セキュリティ設定を「モバイル」とするときのコンピュータ装置の使用環境の一例を示す図である。

【図6】 複数段階のセキュリティ設定の一例を示す図である。

【図7】 セキュリティ設定を初期設定するときの処理の流れを示す図である。

【図8】 PCの使用環境に応じてセキュリティ設定を変更するときの処理の流れを示す図である。

##### 【符号の説明】

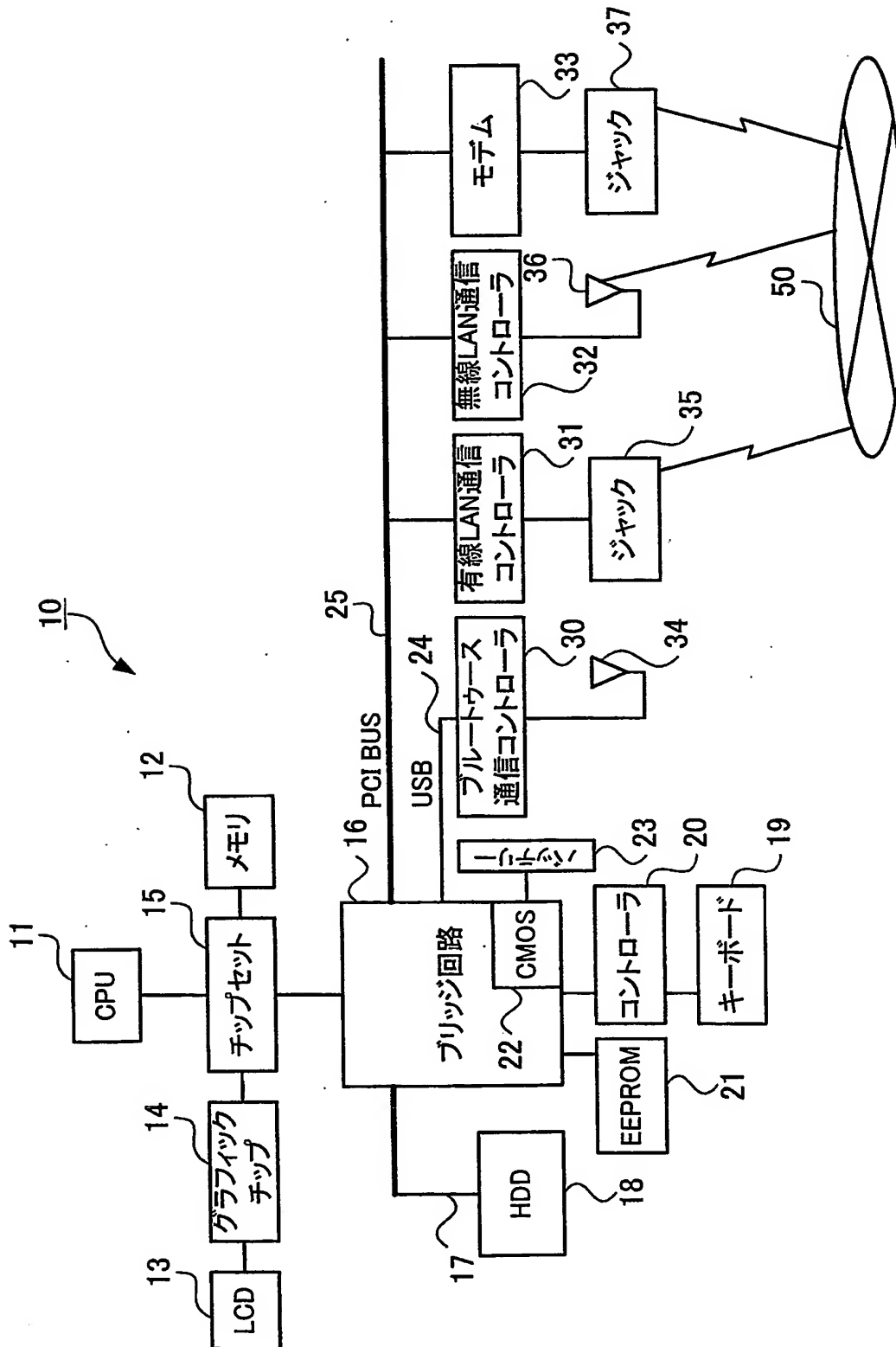
10…PC(コンピュータ装置)、30…ブルートゥース通信コントローラ(識別情報取得手段、通信手段)、40…環境判定部(使用環境判定手段)、41…通信

設定制御部、42…セキュリティ設定制御部(設定変更手段)、43…省電力設定  
制御部(設定変更手段)、44…セキュリティ設定情報格納部

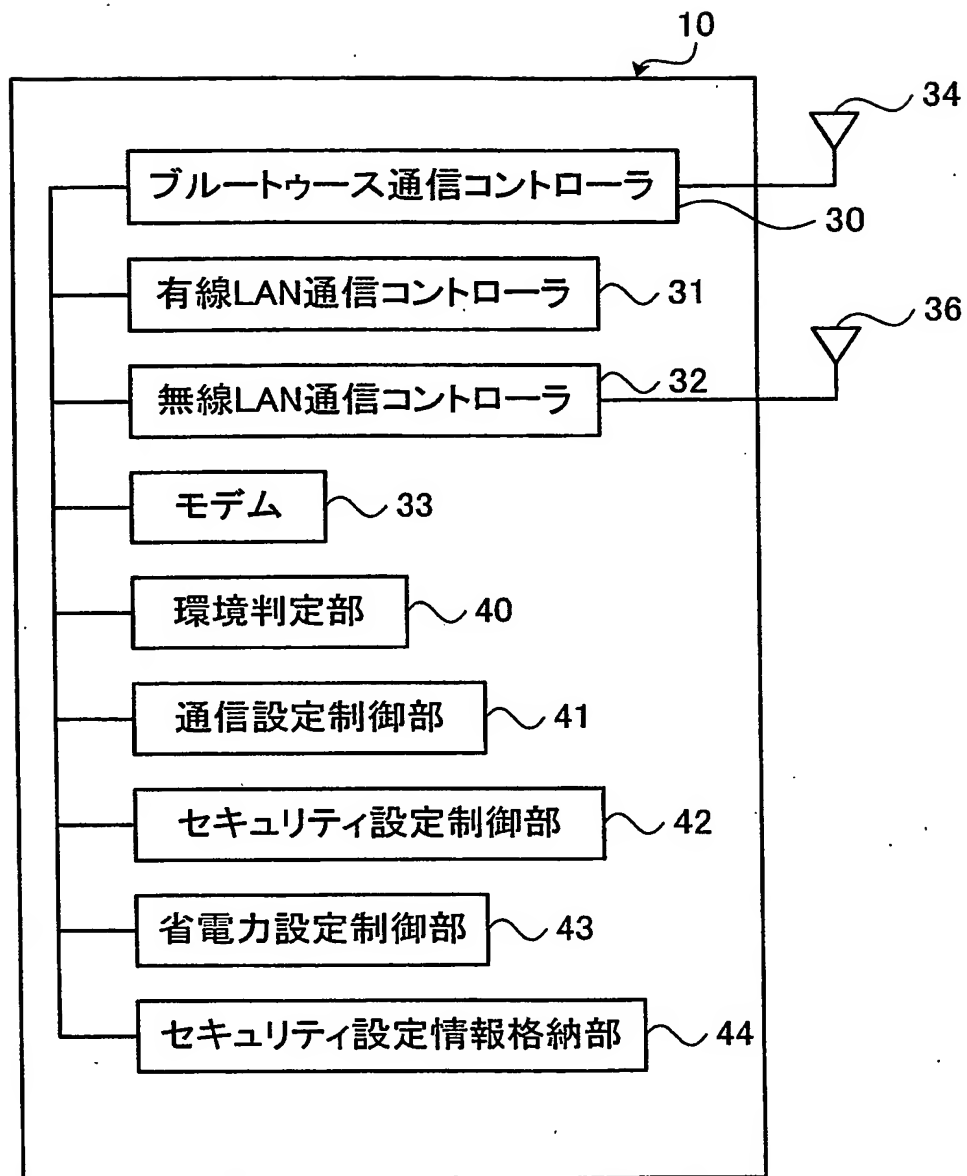
【書類名】

図面

【図1】

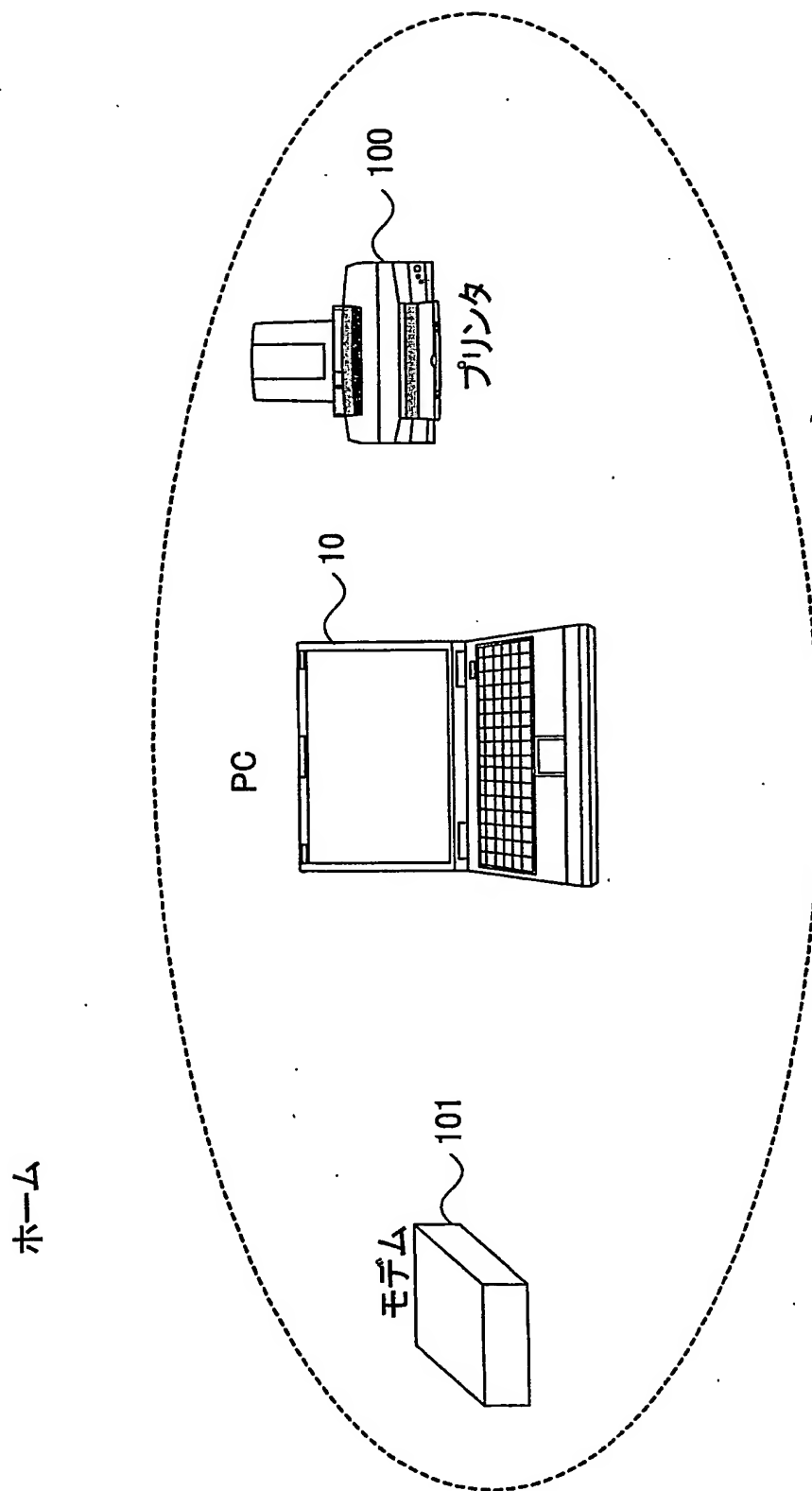


【図 2】

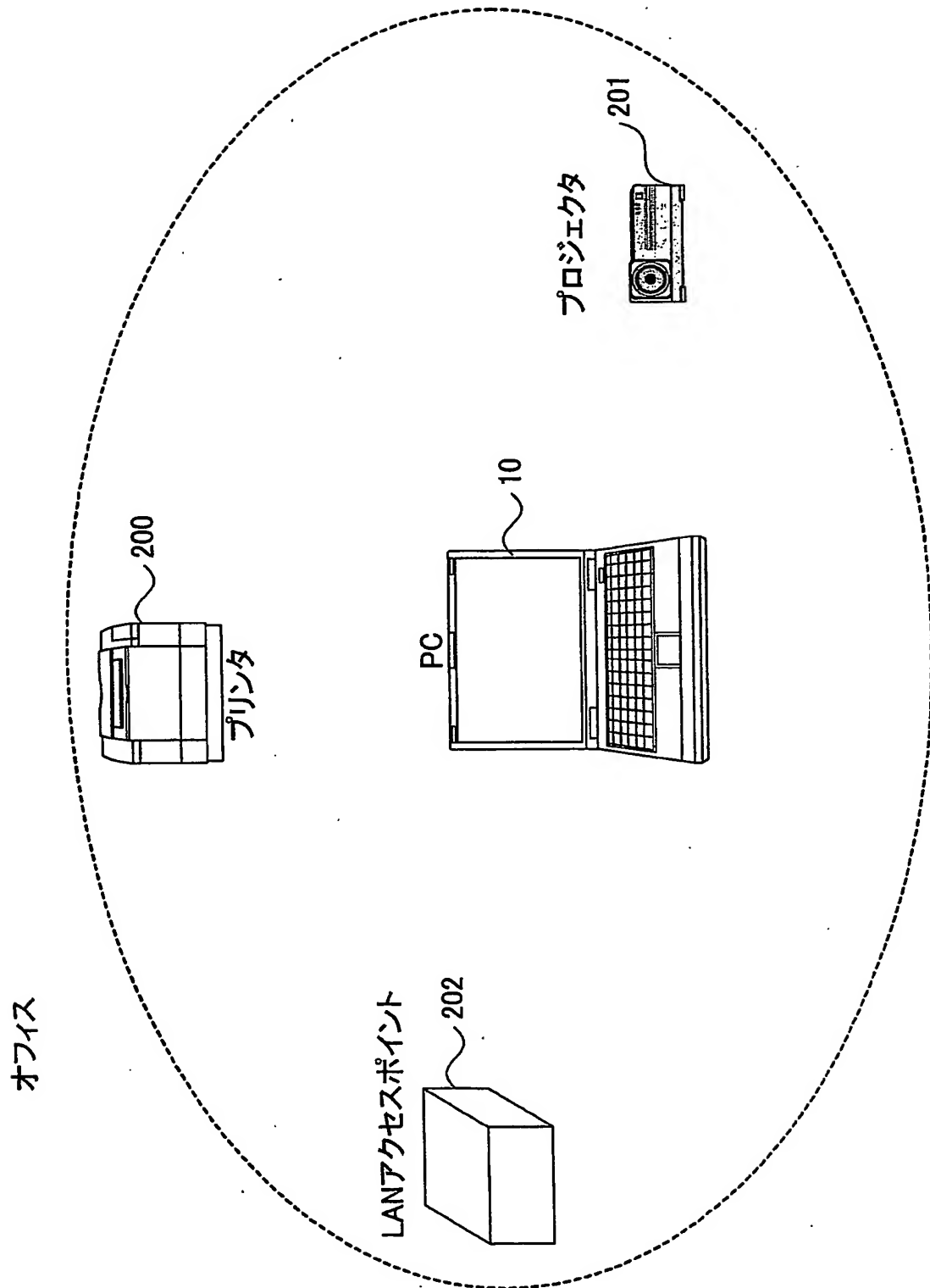




【図3】

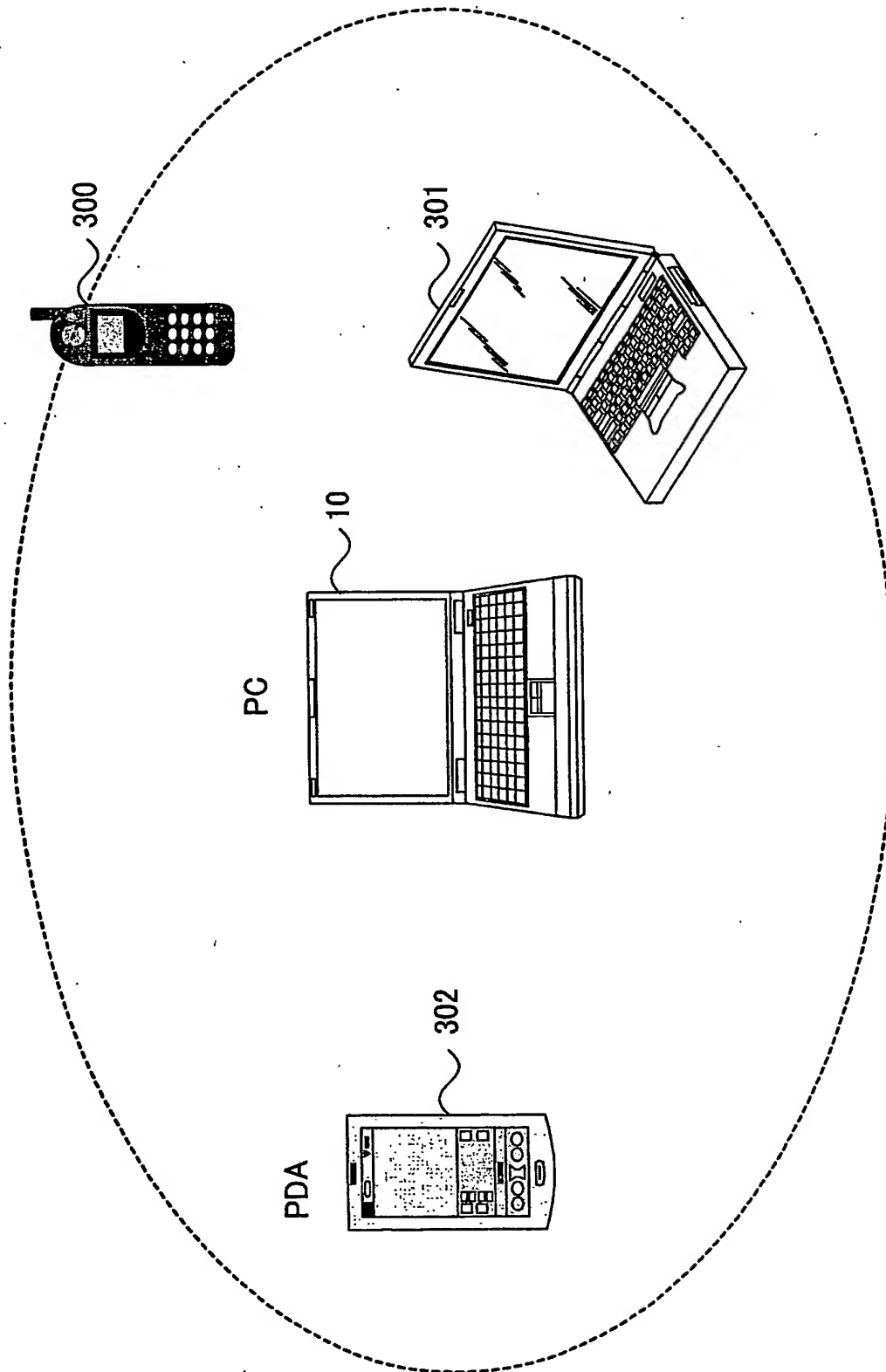


【図4】



【図5】

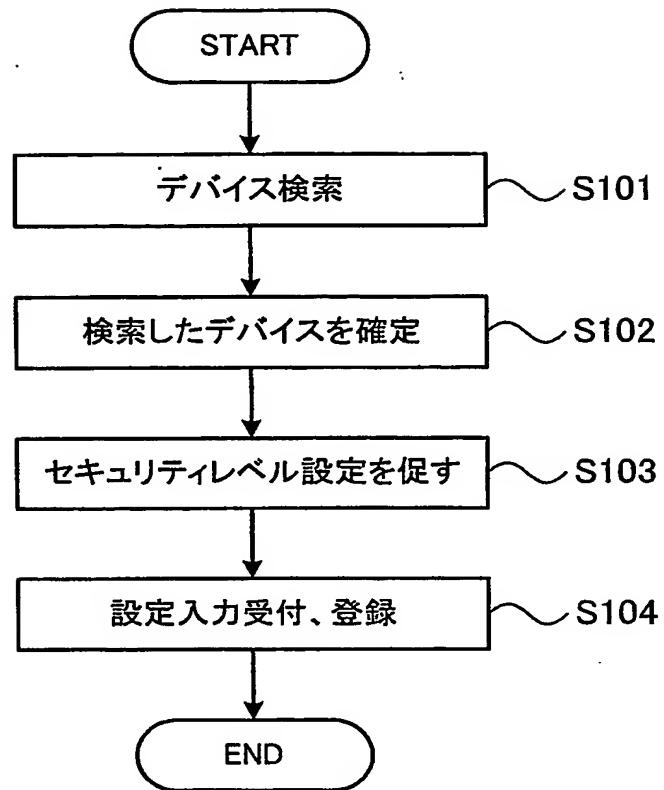
モバイル



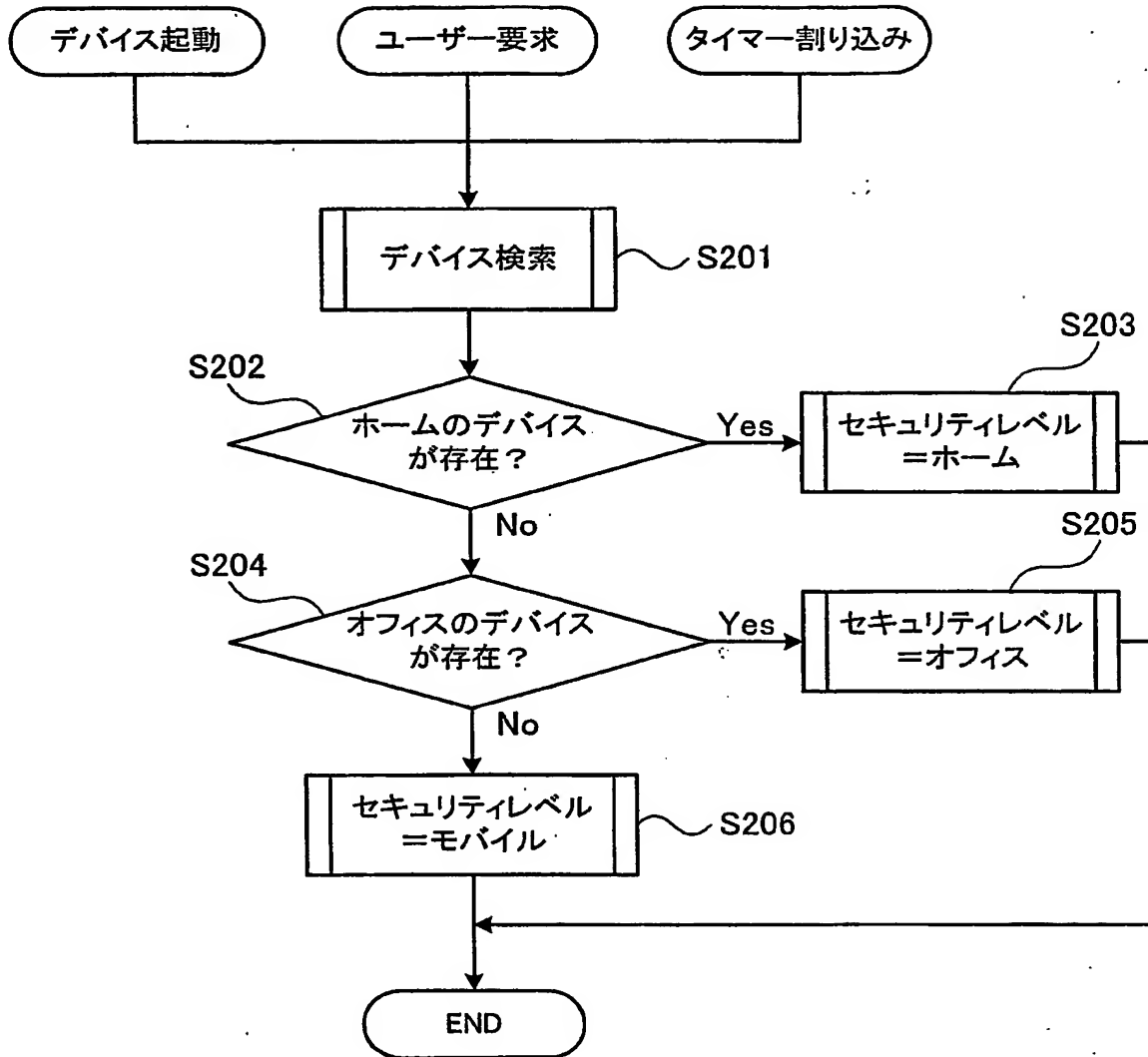
【図6】

| セキュリティ<br>レベル | 他のデバイスからの接続 |    |     | 他のデバイスへの接続 |          |
|---------------|-------------|----|-----|------------|----------|
|               | 認証          | 許可 | 暗号化 | 認証・許可      | 暗号化      |
| ホーム           | 必須          | —  | 必須  | 要求があったとき   | 要求があったとき |
| オフィス          | 必須          | 必須 | 必須  | 要求があったとき   | 要求があったとき |
| モバイル          | 拒否          |    |     | 必須         | 必須       |

【図 7】



【図8】



【書類名】 要約書

【要約】

【課題】 使用環境に応じて確実に設定変更を行うことのできる技術を提供し、セキュリティ性の高いネットワーク接続環境を常に確保する。

【解決手段】 PCでは、ブルートゥースを用い、周辺に存在するデバイスのBDアドレスを検索することによって、PCの使用環境を判定し、その使用環境に応じてセキュリティレベルの設定を自動的に変更するようにした。さらに、使用環境を判定する処理において、セキュリティレベルを「ホーム」や「オフィス」とすべき使用環境にPCがあるときであっても、その使用環境に存在すべきデバイスが検出されないときには、セキュリティ性の高い「モバイル」のセキュリティレベルを設定するようにした。

【選択図】 図 8

認定・付加情報

|         |               |
|---------|---------------|
| 特許出願の番号 | 特願2002-109714 |
| 受付番号    | 50200531300   |
| 書類名     | 特許願           |
| 担当官     | 井筒 セイ子 1354   |
| 作成日     | 平成14年 6月 4日   |

<認定情報・付加情報>

【特許出願人】

|          |                                   |
|----------|-----------------------------------|
| 【識別番号】   | 390009531                         |
| 【住所又は居所】 | アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし) |
| 【氏名又は名称】 | インターナショナル・ビジネス・マシーンズ・コーポレーション     |

【代理人】

|          |  |
|----------|--|
| 【識別番号】   | 100086243                                |
| 【住所又は居所】 | 神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 大和事業所内 |
| 【氏名又は名称】 | 坂口 博                                     |

【代理人】

|          |  |
|----------|--|
| 【識別番号】   | 100091568                                |
| 【住所又は居所】 | 神奈川県大和市下鶴間1623番地14 日本アイ・ビー・エム株式会社 大和事業所内 |
| 【氏名又は名称】 | 市位 嘉宏                                    |

【代理人】

|          |  |
|----------|--|
| 【識別番号】   | 100106699                              |
| 【住所又は居所】 | 神奈川県大和市下鶴間1623番14 日本アイ・ビー・エム株式会社大和事業所内 |
| 【氏名又は名称】 | 渡部 弘道                                  |

【復代理人】

|          |                                      |
|----------|--------------------------------------|
| 【識別番号】   | 100104880                            |
| 【住所又は居所】 | 東京都港区赤坂5-4-11 山口建設第2ビル 6F セリオ国際特許事務所 |
| 【氏名又は名称】 | 古部 次郎                                |

【選任した復代理人】

|        |           |
|--------|-----------|
| 【識別番号】 | 100100077 |
|--------|-----------|

次頁有



認定・付加情報（続き）

【住所又は居所】 東京都千代田区岩本町1丁目4番3号 KMビル  
8階 大場国際特許事務所  
【氏名又は名称】 大場 充

出 願 人 履 歴 情 報

識別番号 [390009531]

1. 変更年月日 2000年 5月16日

[変更理由] 名称変更

住 所 アメリカ合衆国10504、ニューヨーク州 アーモンク (番地なし)

氏 名 インターナショナル・ビジネス・マシーンズ・コーポレーション

2. 変更年月日 2002年 6月 3日

[変更理由] 住所変更

住 所 アメリカ合衆国10504、ニューヨーク州 アーモンク ニュー オーチャード ロード

氏 名 インターナショナル・ビジネス・マシーンズ・コーポレーション